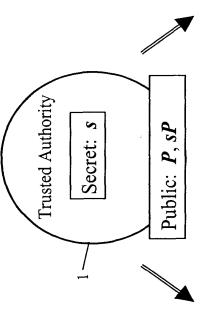
1/4

Figure

(PRIOR ART)



Party B has identity ID and a secret S<sub>ID</sub> from TA where

Non IBC Signatures

Signing by TA:

 $V = sH_1(m)$ 

IBC

 $S_{\text{ID}} = sQ_{\text{ID}}$  and  $Q_{\text{ID}} = H_1 \text{ (ID)}$ 

Encryption by party A Encryption with secret r U = rP

Signing by Party B

Signatures

 $h = H_2(m||r)$ where  $r = t(S_{\text{ID}}, P)^k$ 

 $V = m \oplus H_3(t(sP, rQ_{\mathbb{D}}))$ 

 $m = V \oplus H_3(t(U, S_{\text{ID}}))$ Decryption by party B

Verification by third party Check:  $t(P, V) = t(sP, H_1(m))$ 

Verification by third party

 $U = (k-h)S_{\mathrm{ID}}$ 

 $r' = t(U,P)*t(Q_{\mathrm{ID}},sP)^h$ Check  $h = H_2(m||r')$ 

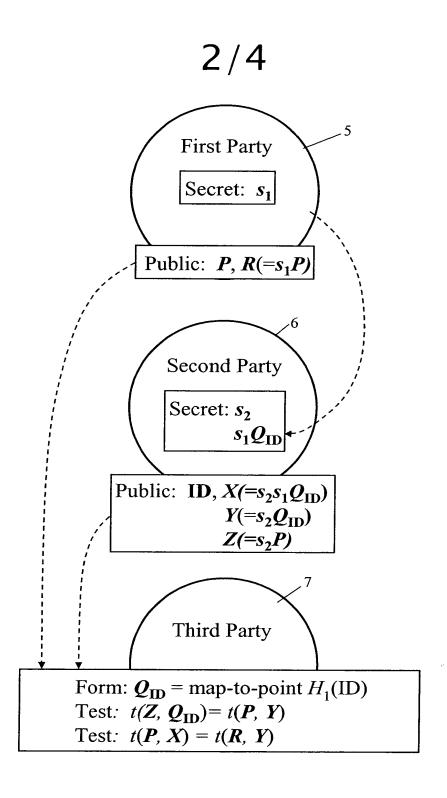


Figure 2

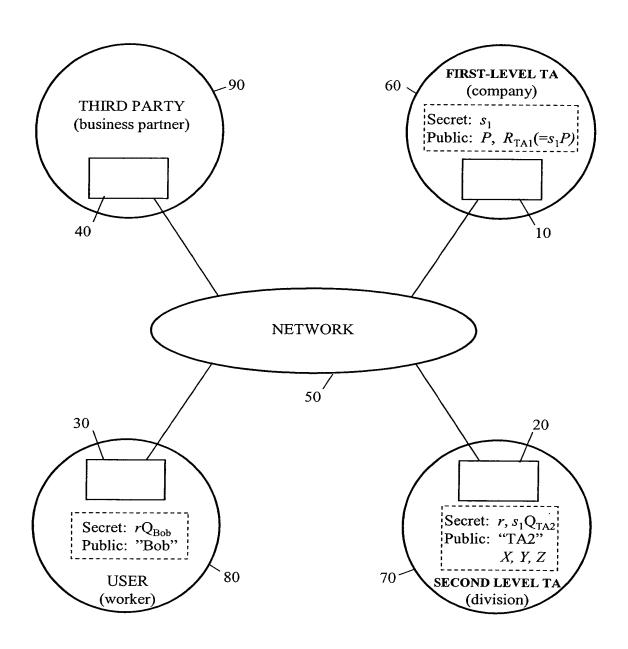


Figure 3

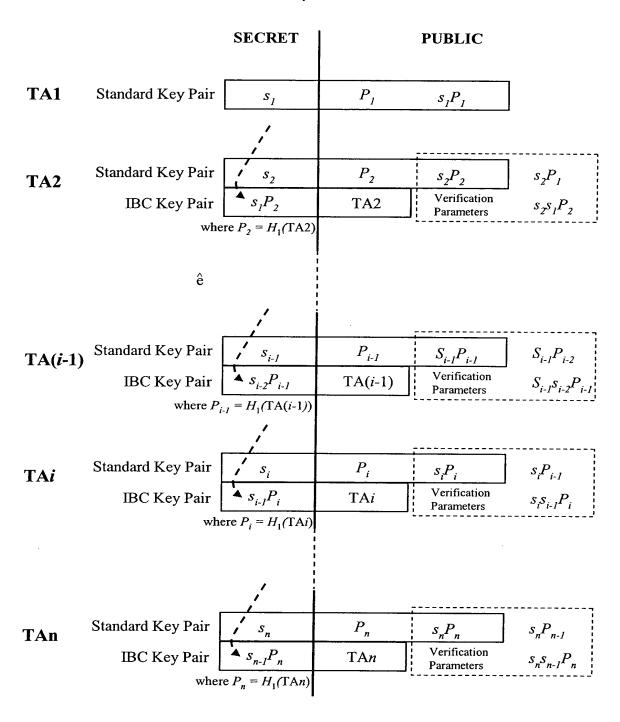


Figure 4